UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

AVAZPOUR NETWORKING SERVICES, INC., JIM AVAZPOUR, and KRISTY AVAZPOUR, Plaintiffs, v. FALCONSTOR SOFTWARE, INC., Defendant.	Civil Action No. CV 12 3574 **COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Avazpour Networking Services, Inc. ("ANS"), founded by Plaintiffs Jim and Kristy Avazpour, is a small business based in Overland Park, Kansas that provides information technology ("IT") services. Together, Plaintiffs, by their counsel, assert claims under New York common law against Defendant FalconStor Software, Inc. ("FalconStor")—a New York-based provider of data-protection and storage-"virtualization" products and services[1]—stemming from FalconStor's improper conduct leading up to, and in performing, an upgrade of ANS's Storage Area Network ("SAN")[2] that began on July 13, 2010 and ended—disastrously—on July 22, 2010. As detailed below, FalconStor's reckless actions in connection with the upgrade led to a failure of ANS's SAN that caused Plaintiffs to suffer significant damages.

[1] Data "virtualization" is premised on the aggregation of data contained within a variety of sources—such as databases, applications, file repositories, websites, and data-service vendors—to provide a single point of access to the data, which can then be used by applications, dashboards, portals, etc.

[2] A SAN consists of a collection of computers and storage devices that are connected over a high-speed optical network and are dedicated to storing and protecting data.

Plaintiffs' claims are made on information and belief (except as to allegations specifically pertaining to Plaintiffs and their counsel, which are made on personal knowledge) based on an investigation conducted by, and under the supervision of, Plaintiffs' counsel. Plaintiffs' allegations are supported by, among other things, documents and other materials from before, during, and after the July 2010 failure of ANS's SAN, as well as by the analysis of a consulting expert specializing in file systems, storage systems, virtualization systems, and operating systems, who concluded that, in conducting the ANS upgrade, FalconStor recklessly disregarded appropriate practices in the data-security and storage-virtualization industry.

NATURE OF THE ACTION

1. This case arises from the misconduct of FalconStor—a provider of data-protection and storage-virtualization products and services that describes itself as "lead[ing] the way in developing innovative, scalable, and open network storage solutions designed to optimize the storage, protection, efficiency, and availability of enterprise data and applications"[3]—in planning for and performing a July 2010 upgrade of ANS's SAN, which FalconStor had recommended to ANS.

2. As detailed below, FalconStor's actions in connection with the upgrade were improper in two major respects. First, in coordinating with ANS to prepare for the upgrade—and then well into the actual upgrade process—FalconStor failed to inform ANS that the hardware FalconStor recommended, and ultimately used, for the upgrade did not support a critical feature of ANS's then-existing network capabilities. Second, in performing the upgrade, FalconStor recklessly disregarded Plaintiffs' rights by eschewing appropriate standards in the data-security and storage-virtualization industry. Among other things, FalconStor used ANS's

[3] See www.falconstor.com/company/about-falconstor/corporate-profile, last visited on July 16, 2012.

SAN as a virtual laboratory for trying untested methods and code to attempt to resolve problems that arose during the upgrade and, perhaps most egregiously, disregarded ANS's *express instruction*—which was consistent with standard practice in the data-security and storage-virtualization industry—that FalconStor should refrain from rebooting the SAN until ANS cleanly shut down its systems. FalconStor's actions in connection with the upgrade were, at a minimum, grossly negligent.

3. Because of FalconStor's misrepresentations before and during the upgrade and its reckless mishandling of the upgrade process, ANS's system sustained operating disruptions on July 20, 2010 and in the following days. As a result of that system failure, ANS clients experienced severe interruptions of their ability to access important network applications—as well as corruption of their data—precipitating a crisis in confidence that led numerous clients to demand credits to their accounts and/or to terminate ANS as their IT-service provider.

4. Plaintiffs have never recovered from the harm FalconStor caused. In addition to losing the existing and potential revenues of customers who abandoned ANS due to the technical disaster that ensued during the upgrade, ANS had to devote considerable time and resources to rehabilitating its SAN to protect against a similar incident as well as addressing client complaints. Accordingly, ANS was unable to devote that time and those resources to cultivating business partnerships—including the potentially lucrative partnership it already had entered into with major regional telecommunications provider SureWest Communications ("SureWest"), of which FalconStor was well aware. ANS also lost valuable employees and clients to local competitors, who relentlessly inundated the local market with negative propaganda regarding ANS's service quality. Additionally, FalconStor's misconduct has placed Jim and Kristy

Avazpour in dire financial straits, as they are defending lawsuits by creditors for failure to comply with ANS-related financial agreements for which they are subject to personal liability.

5. In short, as a direct and proximate result of FalconStor's gross negligence in causing the July 2010 system failure, ANS—until then a successful enterprise with concrete prospects of significant expansion and revenue growth—now stands at the precipice of bankruptcy, as do the Avazpours personally.

JURISDICTION AND VENUE

6. This Court has jurisdiction over the subject matter of this action under 28 U.S.C. § 1332, because there is complete diversity of citizenship between Plaintiffs—all of whom are citizens of Kansas—and FalconStor, a citizen of New York and Delaware, and the matter in controversy exceeds the sum or value of $75,000, exclusive of interest and costs.

7. This Court has personal jurisdiction over FalconStor by virtue of FalconStor's business activities in this jurisdiction. Additionally, the April 22, 2010 "Evaluation Agreement" between ANS and FalconStor, by which FalconStor provided products to ANS that would be used for the July 2010 upgrade, states "[t]he parties agree that any action arising under or relating to this Agreement or the Software shall lie within the exclusive jurisdiction of any State or Federal court located in the State of New York."

8. Venue in the Eastern District of New York is proper under 28 U.S.C. § 1391(b)(1), as FalconStor resides in this District. Venue is also proper under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

THE PARTIES

Plaintiffs

9. Plaintiff Avazpour Networking Services, Inc., founded in 1997, is a small Kansas corporation, based in Overland Park, Kansas, that provides IT services. Though it now services only a few clients, at the time FalconStor began the upgrade of ANS's SAN in July 2010, ANS handled the networking needs of more than 50 small or medium-sized businesses, offering, among other things, complete/hybrid cloud computing, managed hosting, collocation, data protection, disaster recovery and security services. ANS professionals designed, built, and maintained IT systems, allowing ANS clients to focus on their own business needs without the distraction of maintaining IT resources.

10. Plaintiff Jim Avazpour, a citizen of Kansas, is President of ANS and formerly served as both President and CEO of the company. He and his wife, Plaintiff Kristy Avazpour—also a citizen of Kansas—founded ANS, and Kristy Avazpour served as ANS's Vice President of Marketing from 2006 to approximately October 2010.

11. In accordance with an agreement between Jim Avazpour, ANS, and the company's current majority shareholder Technology Capital Investors 4 LLC, Jim Avazpour is authorized to pursue ANS's claims against FalconStor on ANS's behalf.

Defendant

12. Defendant FalconStor Software, Inc., a Delaware corporation founded in 2000, develops, manufactures, and distributes network-storage "solutions" and provides related maintenance, engineering, and implementation services. FalconStor maintains its headquarters at 2 Huntington Quadrangle, Suite 2S01, Melville, New York 11747. In its 2011 Annual Report (Form 10-K) filed with the U.S. Securities and Exchange Commission ("SEC") on or about March 13, 2012, FalconStor described itself as "the market leader in disk-based data protection,"

whose "mission" is "to transform traditional backup and disaster recovery (DR) into next-generation service-oriented data protection."[4] FalconStor also reported that it had 468 full-time and part-time employees as of December 31, 2011 and generated revenues of $82.871 million for 2011, slightly more than its 2010 revenues of $82.844 million.[5]

13. By the spring of 2010, when FalconStor and ANS were contemplating an upgrade of the latter's SAN, FalconStor offered several data-protection and storage-virtualization "solutions": (i) FalconStor© Network Storage Server ("NSS"), for storage virtualization, provisioning, and management—in its 2009 Form 10-K filed with the SEC on or about March 12, 2010, FalconStor stated NSS "integrates storage virtualization and provisioning across multiple disk arrays and connection protocols for an easy-to-use, scalable SAN solution" and "is designed to meet all of the storage needs of any organization"; (ii) FalconStor© Virtual Tape Library ("VTL"), for tape-backup optimization—FalconStor described VTL as "the industry's leading virtual tape solution," further stating, "[w]ith virtual tape, backups complete faster and more reliably, with little or no change needed to the backup environment"; (iii) FalconStor© Continuous Data Protector ("CDP"), for unified backup and disaster recovery—according to the company, CDP "combines local and remote protection into a cost-effective, unified, disk-based solution that allows organizations to recover data back to the most recent transaction"; and (iv) FalconStor© File-interface Deduplication System ("FDS"), for storage-capacity optimization—FalconStor stated FDS "extends FalconStor's deduplication technology to service

[4] FalconStor 2011 Form 10-K at 4.

[5] *Id.* at 13, 31.

a broader set of applications that goes beyond tape backup applications" and "allows companies to optimize storage capacity services for disk-to-disk backup and archiving applications."[6]

14. FalconStor's products and solutions were (and still are) built on its IPStor© "common network infrastructure software platform," which, according to FalconStor, "provides the most reliable and complete disk-based data protection and storage virtualization solutions." According to the company, its data-protection solutions "accelerate or eliminate the backup window, which allows users to recover data in minutes, anytime, anywhere, with 100% data integrity."[7]

ADDITIONAL FACTUAL ALLEGATIONS AS TO FALCONSTOR'S LIABILITY

A. Relying on FalconStor's expertise and recommendations, ANS engaged FalconStor to implement an upgrade of ANS's data-storage infrastructure.

1. ANS depended on FalconStor to support ANS's needs with respect to data security, integrity, and availability, which were critical to ANS's business.

15. As an IT-service provider, ANS places great importance on protecting its clients from service disruptions and, even worse, loss of those clients' data. Clients typically have little tolerance for unscheduled downtime of their networks or persistent problems with poor IT performance. And a major IT incident such as data loss or corruption will severely undermine clients' confidence in an IT provider—which, in the competitive IT-services industry, can quickly cause the provider to lose clients (who will change providers) and suffer lower earnings potential (as the provider's damaged reputation alienates potential clients). Data security and availability thus were central to ANS's ability to meet its clients' needs, and to ANS's financial performance and prospects.

---

[6] FalconStor 2009 Form 10-K at 5-7.

[7] *Id.* at 5.

16. FalconStor has acknowledged the potentially devastating effects of system downtime. In its 2011 Annual Review, for instance, FalconStor's President and CEO James McNiel observed, "No business large or small can tolerate downtime. With an event that shuts down even a part of the data center, there is a great cost that mounts with every hour that passes before full recovery."[8] FalconStor further emphasized, "More than ever, any kind of disruption to data access has a direct and significant impact on business operations and revenue. To ensure business continuity, an organization must prevent service interruptions caused by software or hardware failures."[9] Accordingly, among its "solutions" for businesses seeking to protect against system disruptions, FalconStor offers "a high-availability 'always-on' approach that ensures that all of the components of a storage infrastructure are redundant, and seamlessly redirects access to alternate data sources if necessary."[10]

17. To help secure its clients' data, ANS relied on FalconStor's products and guidance. By 2010, ANS had been a FalconStor customer for approximately six years.

18. In early 2010, having experienced periodic outages of its SAN, ANS approached FalconStor about the prospect of upgrading the SAN. ANS's objectives—as stated in a "Solution Objective Worksheet" ANS provided to FalconStor on May 27, 2010—included "[n]o business interruption or client downtime" and "[n]oticeable performance gains."

19. Beyond generally desiring improved performance for its existing clients, ANS wanted to protect its potentially lucrative relationship with SureWest—"a leading integrated communications provider" that "offers bundled residential and commercial services in the

[8] FalconStor 2011 Annual Review at 2.

[9] *Id.* at 5.

[10] *Id.*

greater Sacramento and Kansas City regions that include IP [Internet Protocol]-based digital and high definition television, high speed internet, Voice over IP, and local and long distance telephone"[11]—with whom ANS had executed an exclusive partnership agreement in 2009 providing that SureWest would sell ANS's IT-outsourcing services, under SureWest's brand, to local businesses. Because a successful relationship with SureWest depended heavily on ANS's service quality and reputation, ANS reasonably believed that enhancing its system performance would render its services more attractive to prospective SureWest customers.

20. FalconStor knew of ANS's business relationship with SureWest. Indeed, FalconStor stood to benefit directly from that relationship, as FalconStor and ANS entered into a "Managed Service Provider Agreement" on January 13, 2010 providing that (among other things) ANS would pay fees to FalconStor in exchange for the right to use FalconStor hardware and software products in servicing SureWest customers. Following the parties' execution of that agreement, Jim Avazpour informed ANS's customers, in a March 1, 2010 e-mail, of the "great news" that ANS had "reached a three year strategic partnership agreement" with FalconStor, which would allow ANS "to leverage its thirteen years of successful experience in IT managed and outsourcing service to aggressively penetrate the growing market demand for Cloud-based services in the SMB [small-and-medium-sized-business] market nationwide."

[11] *See* July 2, 2012 press release issued by Consolidated Communications (which recently acquired SureWest) titled "Consolidated Communications Completes Acquisition of SureWest Communications, located at http://ir.consolidated.com/releasedetail.cfm?ReleaseID=688516, last visited on July 16, 2012.

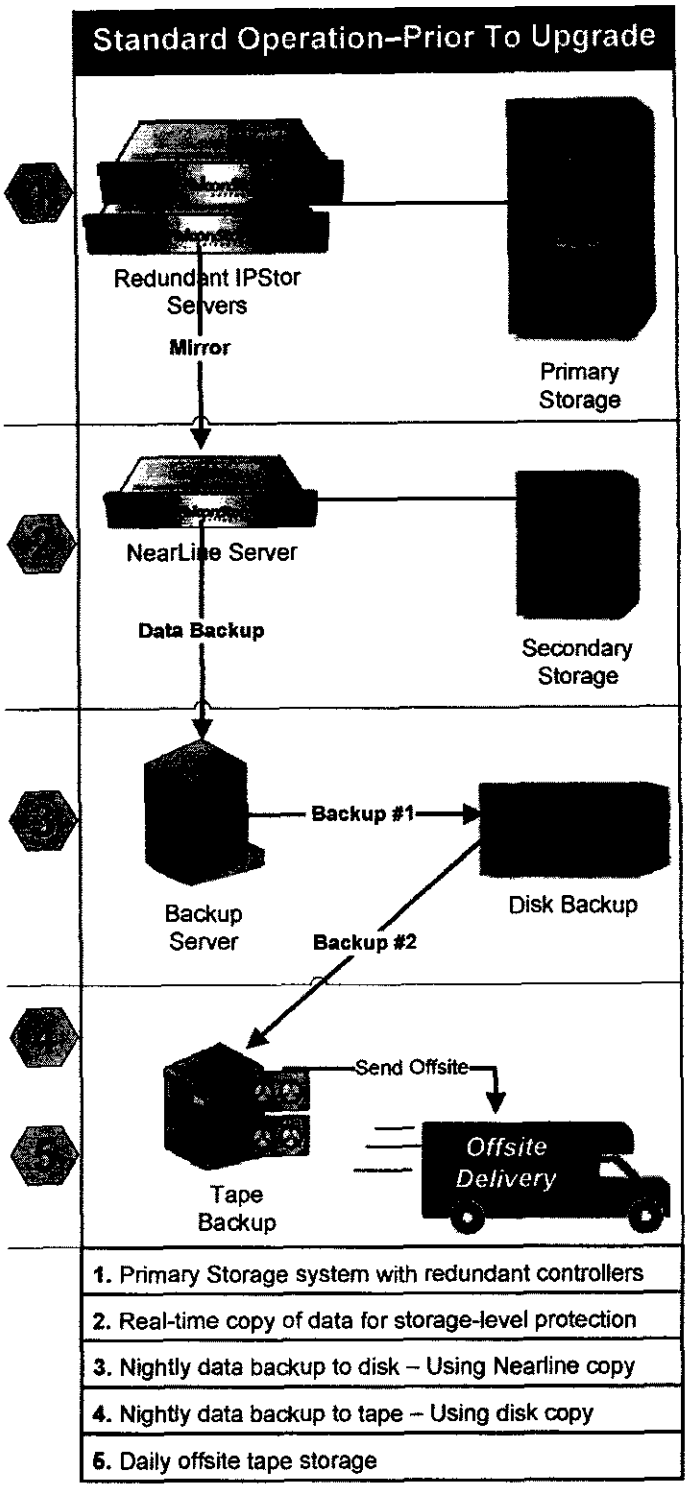
2. In preparing for the upgrade of ANS's SAN—which FalconStor recommended—Jim Avazpour and other ANS personnel provided FalconStor representatives with substantial information about ANS's existing SAN and its objectives for the upgrade.

21. Before the upgrade, ANS's storage system—depicted in the diagram below—included (i) two servers running FalconStor's IPStor version 5 storage-virtualization software, connected to a "production" SAN that contained the actual live data then in use on ANS's network; (ii) a "nearline mirror" server running IPStor version 5, connected to a backup SAN; and (iii) multiple backup servers.[12] Each time data were written to the production SAN, they were also written to the backup SAN through a process known as "nearline mirroring." That contemporaneous writing of data to both SANs promoted data "redundancy"—i.e., where a system component is duplicated so that if it fails, a backup exists. If a problem affected the production SAN, the nearline-mirror server could take the place of the production SAN and continue to serve the production data until the problem was resolved; the nearline-mirror server then would stop serving the production data and would relinquish control to the production SAN.[13] The dynamic between the production SAN and the nearline-mirror server thus provided

[12] In its "IPStor User Guide," FalconStor described IPStor as "an award-winning comprehensive suite of

a valuable "failover" mechanism.[14] Additionally, regular snapshots of data on the backup SAN were taken several times a day and stored there, serving as safe recovery points in the event of data corruption. And data were further protected on both the production SAN and the backup SAN by being stored in a "RAID-5 configuration," in which data were spread across a number of disks in units (called stripes) that include additional "redundant" information (called parity) and allow the data written to any one disk to be computed from the information stored on the remaining disks. Accordingly, the failure of a single disk would not result in data loss. Finally, ANS made nightly tape backups, which were stored off-site.

[14] Failover consists of the capability, upon the failure or abnormal termination of one server, to switch over automatically to a redundant or standby server.



22. ANS thus maintained several safeguards to protect client data in the event of a hardware or software failure. Moreover, having provided data-security products and services to

ANS since 2004, FalconStor was familiar with ANS's existing storage network technology and equipment.

23. In response to ANS's inquiry about a potential upgrade of its SAN, FalconStor recommended that ANS upgrade its existing data-storage infrastructure. FalconStor represented that the new system, which FalconStor was to implement, would provide substantially greater reliability and "availability" than the existing FalconStor products ANS was using. Data "availability" refers to ensuring that data are available at a required level of performance in situations ranging from normal through disastrous. Data availability generally is achieved through redundancy, involving where the data are stored and how the data can be reached.

24. In anticipation of the upgrade, ANS provided details of its existing network/storage environment and requirements to FalconStor. In a March 20, 2010 e-mail, for example, Jim Avazpour informed FalconStor Storage Architect Christopher Mende (and others, including FalconStor's Director of Hosted Services Joe Goldberg and FalconStor's Midwest Territory Account Manager John Martini) that the "plan" was "to replace our current NSS v5.x (HP-based) servers and HP EVA5000 SAN with this new NSS environment." Avazpour added, "The current environment will be upgraded and moved to SureWest datacenter." He further identified ANS's "Requirements": greater reliability and stability, higher availability to meet ANS's duties under its service-level agreements with clients, higher system performance, and compatibility with the network software ANS used—including VMware and SQL Server, which provided for data virtualization.

25. After assessing ANS's needs, FalconStor recommended that ANS upgrade to FalconStor's HC650 SAN appliance with two NSS controllers running a newer version (version 6.15) of the FalconStor IPStor software, which would replace the existing servers that were

running IPStor version 5. In a March 22, 2010 e-mail, for instance, FalconStor's Christopher Mende assured Jim Avazpour that the HC650 was "a good fit for [ANS's] environment" and would "be able to improve on" all of the requirements Avazpour had identified.

26. Consistent with FalconStor's representations to Jim Avazpour, in its "Solution Brochure" FalconStor touted the "Superior Reliability and High Availability" of its HC Series storage platform. Acknowledging "[r]eliability starts with the delivery of highly available platforms offering redundancy and no single point of failure," FalconStor specified: "The active-active controller clustered architecture of the FalconStor HC series provides uninterrupted access to all systems data." Even in the "unlikely" event of a controller failure, FalconStor added, "business operations can continue while the failure is addressed" and "the battery-backed mirrored cache guarantees that no data will be lost due to any controller failure."

27. FalconStor further assured its customers, "All components of the FalconStor HC series platforms are fully redundant and designed to provide greater than 99.999% availability." FalconStor emphasized the HC series' "hardware redundancy" and "additional software features for data protection," which "ensure that data is accessible at all times regardless of any hardware or site failure that may occur."

28. Through the April 22, 2010 "Evaluation Agreement" between FalconStor and ANS, FalconStor provided the HC650 NSS hardware and memory upgrade that were to be used for the ANS system upgrade.

29. In addition to providing the HC650 NSS hardware, FalconStor was to install the hardware and handle the necessary transition from ANS's existing ("old") system environment to the upgraded ("new") environment.

30. In the months leading up to the upgrade, ANS personnel, including Jim Avazpour, detailed to FalconStor representatives how ANS's system worked and described the technological capabilities ANS needed to effectively serve its clients. Among those was nearline mirroring, which (as detailed above) consisted of the contemporaneous writing of the same data to both the production SAN and the backup SAN, promoting data redundancy.

31. Among the information ANS provided to FalconStor in preparation for the upgrade, on June 9, 2010, ANS's Senior Lead Systems Engineer Stephanie Masingale sent to Jon Zhu of FalconStor Professional Services—who was coordinating the ANS upgrade—a diagram illustrating ANS's "data center," which included a depiction of the nearline server. In addition to the diagram, Masingale further noted that ANS's "Engineering HW [hardware] Requirements" included "NSS Running Nearline Up." FalconStor thus was aware that ANS's existing SAN utilized nearline mirroring and that ANS required nearline mirroring in the upgraded SAN.

32. Indeed, the "Statement of Work" FalconStor prepared for the upgrade, in detailing "the specific tasks [sic] items" FalconStor was to perform, stated, among other things, that FalconStor would install two of its CDP 6.15 appliances as well as "configure NLM"—nearline mirroring—"on 2-3 LUNs from NSS [FalconStor's Network Storage Server] to CDP [FalconStor's Continuous Data Protector], and show customer the process."

33. Similarly, during a July 6, 2010 meeting involving Jim Avazpour, Stephanie Masingale, ANS's IT Operations Coordinator Tareek Razack, and FalconStor's John Zhu, Zhu represented to the ANS personnel that he would "replicate a Nearline mirror resource."

34. Even *during the actual upgrade process*, Zhu represented that FalconStor would establish nearline mirroring in the upgraded SAN. In a July 14, 2010 e-mail to Zhu and his colleague Raymond Zhao (also including ANS personnel), Jim Avazpour stated ANS "would

like to move forward with the following implementation," which would include "[u]tiliz[ing] iSCSI for our nearline replication." Later that day, Zhu responded, "Thanks, Jim and Steph [i.e., Stephanie Masingale]. We are executing the cut over plan now."

35. Contrary to its representations that the upgrade would satisfy ANS's stated objectives—greater reliability and stability, higher availability to meet the company's duties under its service-level agreements with clients, higher system performance, and compatibility with its network software—and the express representations in the Statement of Work and elsewhere about configuring nearline mirroring, the NSS server FalconStor used for the upgrade in fact did not support nearline mirroring, a critical data-security component of ANS's existing SAN. As detailed below, FalconStor did not inform ANS of that key fact until well into the upgrade process, when it was too late for ANS reasonably to instruct FalconStor to discontinue the upgrade.

3. Relying on FalconStor's representations concerning the expected benefits of its system upgrade, ANS relayed those assurances to its customers.

36. Having coordinated for months with FalconStor to help ensure that the upgrade would, as FalconStor represented, "be able to improve on" the requirements Jim Avazpour and his team had identified to FalconStor's representatives, ANS touted the upgrade to its customers and prepared them for the transition to the new SAN.

37. On June 3, 2010, for example, ANS, through its "Customer Care Team," sent an e-mail to its customers—with the subject "Avazpour News - Impending Infrastructure Upgrade to Enhance our Clients' User Experience"—detailing the planned "major storage infrastructure upgrade." ANS explained, "We will be upgrading our current Storage Area Network (SAN) and Fibre Channel (FC) switches to an even more robust and scalable environment." The announcement further stated that while the upgrade would "be a large and complex project," the

migration it entailed would "be completely seamless to [ANS] users." ANS also described the "benefits" its clients would experience as a result of the upgrade: (i) "Higher level of performance and availability when accessing applications," (ii) "Faster transfer of data," (iii) "The management of stored data is enhanced and centralized," and (iv) "Easier scalability for future storage needs."

38. On July 12, 2010, Jim Avazpour sent an e-mail to ANS customers referencing the June 3, 2010 e-mail from ANS's Customer Care Team and stating he was "proud to announce that the installation of this new technology will begin tomorrow [July 13, 2010] and will be completed by Sunday, July 18, 2010." Avazpour further explained:

> This will be a large and complex project, but the migration will be completely seamless to our users. Some small elements of our infrastructure will be moved to the new SAN during our scheduled maintenance window on Wednesday, July 14. The remaining elements, including Avazpour's Exchange databases, will be moved to the new SAN during our scheduled maintenance window on Saturday, July 17, 2010.

Similar to the ANS Customer Care Team's June 3, 2010 e-mail, Avazpour described the "benefits" customers could expect from the upgrade:

- Higher level of performance and availability when accessing files on network drives
- Increased level of performance when accessing Outlook email folders via Citrix
- Faster transfer of data
- The management of stored data is enhanced and centralized
- Easier scalability for future storage needs

39. On July 13, 2010, ANS sent an e-mail informing its clients of an "Anticipated Maintenance Period" to allow for data migration in connection with the upgrade. In that e-mail, ANS referenced the regular "two pre-planned maintenance windows per week: one on

Wednesday evenings and the other on Saturday evenings, between the hours of 9:00 PM CT and 3:00AM CT"—and advised clients of a "Scheduled Maintenance" on July 14, 2010 in connection with the FalconStor upgrade. ANS specified that while the "Anticipated Maintenance Period" might last from 9:00 p.m. on July 14 to 3:00 a.m. the following morning, ANS estimated the maintenance would last only four hours, from 9:00 p.m. on July 14 to 1:00 a.m. on July 15. The e-mail then specified that the "maintenance" would entail "[m]igration of some Files data to new Storage Area Network (SAN)," further noting, "Some but not all Files will be migrated during this Maintenance Window." The e-mail continued, "Any files not migrated during this Maintenance Window will be migrated during the Saturday, July 17, 2010 Maintenance Window. A separate Maintenance Notification will be sent to you on Friday, July 16, 2010."

40. ANS's July 13, 2010 e-mail further informed customers of services that would "**not** be available during the maintenance period," specifying: "Some files stored on H, P, and other network drives will be offline during this period," "You will not be able to open files stored on these drives during the maintenance window," and "You will not be able to save files to these drives during the maintenance window." (Emphasis in original.) ANS recommended that users "save and close any files that are located on the network drives before the Maintenance Window begins." And ANS advised that if a user "need[ed] to work with specific files that are stored on network drives while maintenance [was] in progress," the user should "copy the files to [his or her] local desktop before the Maintenance period begins"; the user could "then work on the files stored on [his or her] desktop and then save the files back to the appropriate network drive after the Maintenance Window has ended." (Emphasis in original.)

41. That e-mail also reiterated the "**Reason for Maintenance & Service Improvements Expected**":

> This migration is to move some of the Files data to [ANS]'s new SAN. The expected benefits provided by moving this Files data to the new SAN is [sic] as follows:
>
> - Higher level of performance and availability when accessing files on network drives
> - Faster transfer of data
> - The management of stored data will be enhanced
> - Easier scalability for future storage needs

ANS further stated, "This maintenance is part of a major [ANS] infrastructure upgrade. It is part of our commitment to maintaining our infrastructure in order to provide a positive user experience."

42. ANS thus appropriately prepared its customers for the upgrade, including the "benefits" FalconStor had represented that ANS and its customers could expect from the upgrade.

43. As noted above, the increased reliability and availability that FalconStor promised to ANS—and that ANS, in turn, touted to its clients—were central to ANS's financial condition and prospects. Indeed, that was borne out when, following the July 2010 network failure and resulting data corruption (detailed below), ANS lost numerous clients, did not attract new clients at the same rate it had previously, and saw its once-promising arrangement with SureWest—from which ANS had expected to generate as much as $5 million in revenues in 2010 alone—disappear.

B. FalconStor recklessly mishandled the ANS system upgrade.

44. ANS personnel coordinated with FalconStor Professional Services to arrange for a FalconStor engineer to implement the upgrade onsite at ANS's offices. The upgrade process began on July 13, 2010.

45. From the outset, the process was plagued by problems, starting when FalconStor copied data from the existing storage system—two servers running IPStor version 5—to the new storage system consisting of an HC650 server with two NSS controllers. That replication operation occupied substantial storage system resources, which degraded the performance of the storage system, leading ANS clients to complain about impaired service. To improve performance, some of the nightly data backup tapes were cancelled, allowing for the dedication of more storage resources to the data-replication process. As a result, ANS was left without nightly backup tapes, which had protected against data loss. While no data yet were lost, the discontinuation of nightly backups—of which FalconStor was contemporaneously aware—necessitated that FalconStor be particularly sensitive to the vulnerable state of ANS's network environment when proceeding with the upgrade.

46. Additionally, during that phase of the upgrade, an inconsistency in configuration between the new storage system and the existing servers became evident: a mismatch in the version of the protocol used to transfer data between the old and new systems (the MTCP protocol).

47. Specifically, FalconStor's IPStor software required that the old system and the new system use the same version of the MTCP protocol to migrate existing client data to the new system. As things then stood, however, on the old system one FalconStor server and the nearline server were using MTCP version 1 and the other FalconStor server was using MTCP version 2, whereas the new system was configured entirely with MTCP version 2. Accordingly, only data

from the one existing FalconStor server with MTCP version 2 could then be replicated to the new system.

48. To rectify the incongruity between the old and new systems, and thus allow the data replication to proceed fully, FalconStor engineer Jon Zhu rolled back both NSS controllers in the new system from MTCP version 2 to version 1. Operating both the old and new systems through MTCP 1 allowed for successful replication of all production data from the old system to the new NSS controllers, but it also delayed the transfer of the nearline server from running on the old system (i.e., with IPStor version 5) to the new system (with IPStor version 6.15). The lack of nearline mirroring left ANS's new system without that pivotal data-protection feature, increasing the company's vulnerability to data loss.

49. The next phase of the upgrade—which could not proceed until July 18, 2010, when all the production data had been successfully replicated from the old system environment to the new NSS controllers—entailed attaching all production servers to the new storage system. That process was completed in the early morning hours of July 18. At that point, all production servers were up and functioning normally, though the nearline server was still running on the old IPStor version 5 system and the data backups on that system began to age, as no new snapshots could be taken until the nearline server was reloaded with IPStor version 6.15 (the newer version) and set up to operate on the new system. FalconStor thus set about upgrading the nearline server from the old IPStor system to the new IPStor system.

50. By the beginning of the nearline-server-conversion phase, no data had been lost, but the upgrade process had disabled many of ANS's normal data-backup and redundancy measures. Data were now being stored in the new system, which included a RAID-6 configuration (a more protective setup than on the old system based on RAID-5), but other

safeguards—such as nearline mirroring and tape backups—were not yet back in place, rendering ANS's system more susceptible to potential data loss in the event of a system failure.

51. As a data-protection provider, FalconStor was well aware of the need to minimize the length of that phase of the upgrade process—and to proceed carefully so as to safeguard ANS clients' data. To the contrary, though, FalconStor recklessly expanded the window of vulnerability when its engineer Jon Zhu left ANS's offices in the early morning of July 18, 2010 and attempted to manage the remainder of the upgrade process remotely. Before his departure, Zhu had attempted to upgrade the nearline server, but he did not wait to determine whether the upgrade was successful. In fact, it was not.

52. Zhu's recklessness in leaving the ANS site without having resolved the nearline mirroring issues unnecessarily, and improperly, exacerbated the already precarious situation at the company. Unable to contact Zhu, ANS engineers spent hours on the phone with FalconStor technical support attempting to resolve problems with the nearline server. FalconStor suggested and implemented a number of incorrect measures to attempt to fix the problems, before finally identifying the root cause: the upgraded software on the newly-loaded nearline server was incompatible with the existing two-gigabit HBA (host bus adapter) cards that had been used on the old system. To resolve that problem, new four-gigabit HBA cards were ordered. After those cards arrived on July 20, 2010, the nearline server was successfully configured and connectivity to the backup SAN was verified.

53. Having finally reached the last stage of the upgrade process, in which FalconStor would attempt to reestablish nearline mirroring (as well as the regular tape-backup schedule) on ANS's new system, FalconStor was still aware the system remained in a fragile state. FalconStor's actions during that phase, though, would prove calamitous.

54. Of central importance in this last phase, to reestablish nearline mirroring, FalconStor had to upgrade both NSS controllers in the new system to MTCP version 2 (Jon Zhu earlier having downgraded them to version 1 to enable data replication). That process, which Zhu conducted remotely, began on July 20, 2010.

55. To create space for nearline mirroring and data snapshots on the new system, ANS had to purge the existing data—including all snapshots of client data going back at least 30 days (which already were outdated by three days)—from the old nearline server. While ANS still could have restored the data in the event of a system failure, that necessary step further reduced the level of data redundancy on the company's system.

56. At that point, one of Jon Zhu's superiors at FalconStor *for the first time* informed Jim Avazpour that the HC650 SAN appliance FalconStor was using for the upgrade—which FalconStor had expressly assured Avazpour would meet ANS's needs—*did not support nearline mirroring*, a critical feature of the company's existing SAN. In light of FalconStor's prior representations about the suitability of its products for ANS's network, the Statement of Work's express reference to "configur[ing] NLM [nearline mirroring]" as part of the planned upgrade, and numerous other representations by FalconStor leading up to—and during—the upgrade process, that revelation stunned Jim Avazpour and others at ANS.

57. In the absence of the nearline-mirroring capability—which served a critical data-security function—FalconStor would have to transfer data from the new system to the old nearline server by replicating the data. While replication provides a mechanism for creating a copy of production data on a backup SAN, it does not possess the automatic failover/failback capability of nearline mirroring. Replication therefore is inferior to nearline mirroring.

58. Nonetheless, given that all of ANS's production data had been moved to the new system and most of the company's data-redundancy safeguards had been disabled to accommodate the system upgrade, ANS reasonably believed it had no choice but to allow FalconStor to proceed with the replication process in order to reestablish the redundancy features that would protect the production data on ANS's system.

59. The replication process would entail upgrading the MTCP on both of the new NSS controllers from version 1 to version 2. To allow ANS's network to run during that upgrade, FalconStor would upgrade one controller at a time; as one was upgraded, the other would handle system operation duties—normally handled by the two controllers working in tandem—itself. Once relieved of its duties, the idle controller could be upgraded and, after the upgrade was complete, could resume its responsibilities.

60. A new problem arose when, after FalconStor upgraded the second controller ("Controller 2")—the first controller ("Controller 1") having been upgraded successfully—Controller 2 was unable to reassume its responsibilities from Controller 1. After unsuccessfully attempting a variety of measures to resolve the issue, FalconStor could have decided at that point to obtain a replacement for Controller 2, as Controller 1 was then handling all system operations. Instead, FalconStor engineers began aggressively trying to force Controller 2 to reassume its duties by *manually applying untested code*, forcing data/resources over to Controller 2 (even though it was not fully functional), and disabling the failover capability between the two controllers.

61. FalconStor ultimately was able to force Controller 2 to reassume its duties, but the controller then did not perform to its usual capacity. For example, Microsoft© Exchange databases that would normally take a few seconds to start took nearly 30 minutes to fully mount

(come online and start), and would then abruptly stop. Controller 2's decreased performance, which continued into July 21, 2010, prevented ANS from keeping its SAN fully available to clients. When ANS attempted to restart nightly backups, the backups proceeded so slowly that all mail clients slowed to a halt.

62. FalconStor's actions up to that point caused ANS's system to remain in an exposed state, increasing the likelihood that any additional mishandling of the system would result in data corruption. Indeed, FalconStor subsequently did just that.

63. On July 21, while still attempting to resolve the problems with Controller 2, FalconStor asked to reboot the system. ANS informed FalconStor that *to prevent data corruption*, it was first necessary to cleanly shut down the servers that were accessing the data on the NSS. In that instance, FalconStor waited for ANS personnel to properly shut down the servers, and the system then was rebooted without data corruption.

64. On July 22, 2010, FalconStor again asked to reboot the system, telling ANS that—contrary to ANS's instruction the previous day—ANS did not need to first shut down the servers. In that instance, though, ANS did (as the day before) shut down the servers before FalconStor rebooted the system.

65. Shortly afterward, however, FalconStor again rebooted the entire system—this time *without warning ANS and without allowing for the necessary shutdown.*

66. FalconStor Professional Support then recommended reseating Controller 2—which would completely shut off power to its circuit board, cache, etc.—and causing the controller to start back up fresh. But once Controller 2 was brought back up, nearly all e-mail databases and file servers were corrupted. Moreover, without nearline mirroring or regular tape backups, which had been disabled to allow for the system upgrade, ANS was left with corrupted

client data and only tape backups that were by then over a week old. Data from the week before the shutdown thus were gone forever.

67. Thus disregarding ANS's clear and unequivocal warning about rebooting the system before allowing for a shutdown, FalconStor—which already had placed ANS's system in a fragile state—caused the irretrievable loss of ANS clients' data. FalconStor's blatant disregard for ANS's instruction contravened standards of the data-security and storage-virtualization industry.

68. Moreover, FalconStor's failure to inform ANS that the HC650 NSS appliance FalconStor had recommended for the upgrade did not support nearline mirroring contributed to the system failure and resulting data loss, because the absence of nearline mirroring both necessitated the replication process that spawned problems with Controller 2 and, in turn, FalconStor's ill-fated attempts to deal with that issue. Additionally, had nearline mirroring been available on the new system, it would have provided a measure of protection against the data loss that ultimately ensued due to FalconStor's reckless disregard of ANS's shutdown instruction.

69. Far from receiving the improved system FalconStor had promised, ANS lost the trust of many of its clients due to the extended system downtime and intermittent system disruptions and, most importantly, the loss of a week's worth of data. Additionally, though the new system was up, it was running in a crippled state until FalconStor replaced Controller 2 the next month. Even then, the new system did not achieve a high-availability state.

C. Expert analysis confirms that FalconStor's conduct in connection with the upgrade evinced a reckless disregard for appropriate practices in the data-security and storage-virtualization industry.

70. Further demonstrating FalconStor's liability, a consulting expert engaged by Plaintiffs—who specializes in advanced computer networking, computer security, virtualization, and file systems—has opined that FalconStor treated ANS's critical production data environment

with reckless disregard for appropriate practices in the data-security and storage-virtualization industry, particularly given FalconStor's detailed knowledge of ANS's existing system and objectives in proceeding with the July 2010 upgrade.

71. The expert further opined that actions FalconStor engineers took during the last phase of the upgrade process to address problems with Controller 2—in particular, applying untested code/"fixes" and rebooting the system without first adhering to ANS's instruction to allow for a clean shutdown—were more suited to a laboratory environment, in which FalconStor could experiment, rather than to a business-critical data facility such as ANS. Moreover, those improper actions came after FalconStor already had rendered ANS's production data more vulnerable to corruption than they ordinarily would have been, given the suspension of tape backups due to the system slowness caused by the upgrade and the inability to reestablish nearline mirroring—an important feature of ANS's old system that FalconStor failed to inform ANS would not be available in the new system FalconStor was implementing.

72. The expert concluded that FalconStor's actions fell well below industry standards, in several respects:

First, FalconStor failed to handle the production data on ANS's SAN with appropriate care in light of the system's vulnerability to data loss due to the disabling of nearline mirroring and other redundancy measures—including by forcing Controller 2 to resume its system duties even though the controller indicated it was unable to do so and by failing to heed ANS's critical instruction that the system be shut down cleanly before rebooting. Sudden reboots without a clean shutdown have a known potential to result in data corruption.

Second, FalconStor failed to minimize the window of the ANS system's vulnerability during which nearline mirroring and regular tape backups were disabled. FalconStor could have limited that period to the time required to rebuild the nearline server.

Third, FalconStor inadequately prepared for the upgrade. Specifically, FalconStor should have estimated the time it would take to replicate data to the new storage system while still maintaining an acceptable level of performance for ANS clients as well as a reasonable backup schedule, and should have identified and resolved system-compatibility issues (e.g., MTCP version 1 vs. MTCP version 2, and the need for four-gigabit HBAs) before beginning the upgrade. FalconStor also should have more carefully assessed the features in use in ANS's existing environment—i.e., nearline mirroring—and informed ANS that the hardware FalconStor

74. Jim Avazpour's IM exchanges with Joe Goldberg continued intermittently over the next couple of days, until the afternoon of July 23, 2010. During that span, ANS fielded complaints and ultimatums from disgruntled customers, including one who, as Avazpour described to Goldberg, was "[d]emanding slash credit, RCA [root-cause analysis], guarantee that it will never happen again, and my 1st b[o]rn."

75. ANS clients' reaction to the system failure FalconStor caused exemplified FalconStor's own observation that "any kind of disruption to data access has a direct and significant impact on business operations and revenue."[15]

76. In addition to losing clients (and thus recurring revenues) that it has not regained, ANS suffered irreparable damage to its reputation, as the corruption of its clients' data—a major setback for a company like ANS, whose business is based on providing high-quality networking services, including data protection—has rendered the company less attractive to potential clients. That reputational damage has translated to lower revenues and decreased earnings potential.

77. Moreover, the extraordinary time and resources ANS was forced to devote to addressing the system problems hindered its ability to pursue other business opportunities. Among other things, as Jim Avazpour foresaw in his IM correspondence with Joe Goldberg at the time of the system failure, ANS's potentially blockbuster arrangement with SureWest imploded—and SureWest ultimately discontinued its relationship with ANS—principally because of ANS's diminished reputation (and thus market share), as well as its inability to expend sufficient time and resources to develop that opportunity, after the events of July 2010. For the same reasons, ANS was constrained from exploring other potential business relationships similar to the agreement it had entered into with SureWest.

---

[15] FalconStor 2011 Annual Review at 5.

78. Attempting to ward off bankruptcy due to the myriad financial ramifications of FalconStor's conduct, in October 2010 Jim Avazpour consummated a sale of a large portion of ANS's stock to Technology Capital Investors 4 LLC, an affiliate of Technology Capital Investors ("TCI"). The purchase price, though, depended on ANS's monthly recurring revenues, which had fallen sharply since the July 2010 system failure. ANS thus did not command remotely as favorable a deal as it would have before FalconStor recklessly harmed ANS's goodwill.

79. Based on an analysis of its revenues from before and after the events of July 2010, ANS values TCI's valuation of ANS in connection with its affiliate's purchase of a large portion of ANS's stock. Plaintiffs estimate ANS has suffered between $5 million and $6 million in lost goodwill value and potential lost revenue—in addition to its potential losses due to the failure of the SureWest deal, on which ANS had projected to make up to $5 million in 2010 alone.

80. Additionally, despite their efforts to mitigate the severe damage FalconStor's misconduct has wrought, ANS, as well as Jim and Kristy Avazpour personally, now face the very real prospect of bankruptcy. ANS's financial condition has not improved, and the company, together with the Avazpours, is the subject of legal proceedings by several creditors to recover millions of dollars based on the alleged failure to comply with certain loan agreements—claims that would not have arisen absent FalconStor's misconduct. ANS also lost the lease on its office space, and Jim and Kristy Avazpour could even lose their home. In all, FalconStor's egregious misconduct with respect to the July 2010 upgrade has caused Plaintiffs to suffer an estimated $37 million in damages.

CLAIMS FOR RELIEF

FIRST CLAIM FOR RELIEF

Gross Negligence

Asserted by All Plaintiffs

81. Plaintiffs incorporate by reference and reallege the preceding allegations as though fully set forth herein.

82. FalconStor had a duty, in advising Plaintiffs about a potential upgrade of ANS's SAN, to act with reasonable care, including adequately examining ANS's existing SAN and determining that the FalconStor products and "solutions" it recommended for the upgrade were suitable for ANS's business needs.

83. In the months leading up to the July 2010 upgrade, ANS provided ample information to FalconStor concerning ANS's SAN—including its nearline-mirroring feature—and the company's objectives for the upgrade.

84. FalconStor understood that ANS expected the upgraded SAN would include nearline mirroring. Indeed, among the numerous representations FalconStor made to ANS both before and during the upgrade process, the Statement of Work FalconStor prepared before the upgrade stated FalconStor would, among other things, "configure NLM [nearline mirroring] on 2-3 LUNs from NSS [FalconStor's Network Storage Server] to CDP [FalconStor's Continuous Data Protector]."

85. FalconStor continually either affirmatively misstated or failed to inform Plaintiffs, until July 20, 2010, that the hardware FalconStor intended to, and did, use for the upgrade did not support nearline mirroring.

86. FalconStor also had a duty, in performing the upgrade, to treat ANS's SAN with appropriate care and to otherwise adhere to standards of the data-security and storage-virtualization industry.

87. FalconStor, in grossly negligent fashion, breached its duties to Plaintiffs in at least two respects. First, in coordinating with ANS to prepare for the upgrade, and even well into the actual upgrade process, FalconStor failed to inform ANS that the HC650 NSS appliance FalconStor intended to, and ultimately did, use for the upgrade did not support nearline mirroring. Second, in performing the upgrade, FalconStor failed to exercise even slight care or diligence, or recklessly disregarded Plaintiffs' rights, by eschewing appropriate standards in the data-security and storage-virtualization industry. Among other things, FalconStor recklessly used ANS's SAN as a virtual laboratory for trying untested methods and code to attempt to resolve the problems that affected Controller 2 during the upgrade and, even worse, disregarded ANS's express instruction to refrain from rebooting the SAN until ANS cleanly shut down its systems.

88. As a direct and proximate result of FalconStor's grossly negligent breaches of the duties it owed to Plaintiffs, Plaintiffs have suffered significant damages. The system downtime and data loss that FalconStor's improper actions precipitated caused ANS to lose clients, potential revenues, and employees—including due to SureWest's discontinuation of its partnership with ANS—and have ruined ANS's reputation. In short, FalconStor's misconduct has driven ANS to the brink of bankruptcy. Additionally, Jim and Kristy Avazpour (as well as ANS) are being sued by creditors for failure to comply with ANS-related financial agreements for which they are subject to personal liability.

89. Plaintiffs timely bring this claim against FalconStor to seek relief for the damages FalconStor's gross negligence has caused.

90. Plaintiffs therefore are entitled to damages in an amount to be proven at trial.

SECOND CLAIM FOR RELIEF

Negligent Misrepresentation

Asserted by All Plaintiffs

91. Plaintiffs incorporate by reference and reallege the preceding allegations as though fully set forth herein.

92. As a professional engaged in a business relationship with ANS that placed the two entities in privity with each other or so close as to approach privity, FalconStor had a duty, in advising ANS about a potential upgrade of ANS's SAN, to impart correct information to ANS—including with respect to whether the products and "solutions" FalconStor recommended for the upgrade would satisfy ANS's business needs and technical requirements, such as nearline mirroring.

93. In preparing for the upgrade, FalconStor (i) represented to ANS (through its President and then-CEO Jim Avazpour) that the products FalconStor had recommended would satisfy ANS's stated objectives—greater reliability and stability, higher availability to meet the company's duties under its service-level agreements with clients, higher system performance, and compatibility with its network software; and (ii) expressly represented that ANS's upgraded SAN would include nearline mirroring.

94. Contrary to those representations, the HC650 NSS server FalconStor used for the upgrade did not support nearline mirroring, a critical data-security component of ANS's existing SAN. FalconStor did not inform ANS of that key fact until well into the upgrade process, when it was too late for ANS reasonably to instruct FalconStor to discontinue the upgrade.

95. In addition to its affirmatively false or misleading statements, FalconStor omitted to inform ANS during the period leading up to the upgrade—and indeed, well into the upgrade process—that the HC650 NSS server FalconStor intended to, and ultimately did, use for the upgrade did not support nearline mirroring.

96. ANS relied on FalconStor's misstatements or omissions.

97. ANS's reliance was reasonable, particularly given that FalconStor possessed unique or specialized expertise in data security and storage virtualization and had detailed knowledge of ANS's SAN.

98. ANS's reliance was foreseeable by FalconStor, in light of (i) FalconStor's longstanding business relationship with ANS, (ii) FalconStor's coordination with ANS regarding the upgrade, and (iii) FalconStor's unique or specialized expertise in data security and storage virtualization.

99. As a direct and proximate result of FalconStor's misconduct, ANS experienced a devastating system failure and loss of client data, which in turn caused Plaintiffs to suffer significant damages.

100. Plaintiffs timely bring this claim against FalconStor to seek relief for the damages FalconStor's negligent misrepresentations have caused.

101. Plaintiffs therefore are entitled to damages in an amount to be proven at trial.

THIRD CLAIM FOR RELIEF

Breach of Contract (due to gross negligence)

Asserted by Plaintiff Avazpour Networking Services, Inc.

102. Plaintiffs incorporate by reference and reallege the preceding allegations as though fully set forth herein.

103. The Statement of Work for the July 2010 upgrade described "the work to be performed" for ANS by FalconStor. The work FalconStor contracted to perform included "Appliance Installation," which entailed, among other things, "configur[ing] NLM"—nearline mirroring—"on 2-3 LUNs from NSS [FalconStor's Network Storage Server] to CDP [FalconStor's Continuous Data Protector]."

104. FalconStor breached its obligations under the Statement of Work when, through its gross negligence, it failed to configure nearline mirroring on ANS's SAN as part of the upgrade.

105. As a direct and proximate result of FalconStor's breach, ANS experienced a devastating system failure and loss of client data, which in turn caused Plaintiffs to suffer significant damages.

106. Plaintiffs timely bring this claim against FalconStor to seek relief for the damages FalconStor's breach of contract has caused.

107. Plaintiff ANS therefore is entitled to damages in an amount to be proven at trial.

FOURTH CLAIM FOR RELIEF

Breach of the Implied Covenant of Good Faith and Fair Dealing

Asserted by Plaintiff Avazpour Networking Services, Inc.

108. Plaintiffs incorporate by reference and reallege the preceding allegations as though fully set forth herein.

109. Through the April 22, 2010 Evaluation Agreement, FalconStor provided products that it intended to, and ultimately did, use for the upgrade of ANS's SAN in July 2010. FalconStor's obligations under the Evaluation Agreement included the covenant—implied in every contract—to exercise good faith in planning for the upgrade and to deal fairly and in good faith with ANS in doing so.

110. The HC650 NSS server FalconStor provided to ANS in connection with the Evaluation Agreement, and then used for the upgrade, did not support nearline mirroring, a critical data-security component of ANS's existing SAN—which, as FalconStor knew, ANS reasonably expected would be included in its upgraded SAN. FalconStor did not inform ANS until well into the upgrade process (when it was too late for ANS reasonably to instruct FalconStor to discontinue the upgrade) that the HC650 NSS product FalconStor had provided for the upgrade did not support nearline mirroring. FalconStor thus breached the implied covenant of good faith and fair dealing in the Evaluation Agreement.

111. Additionally, and separate from the Evaluation Agreement, the Statement of Work for the July 2010 upgrade described "the work to be performed" for ANS by FalconStor. FalconStor's obligations under the Statement of Work included the covenant—implied in every contract—to exercise good faith in performing the upgrade and to deal fairly and in good faith with ANS during that process.

112. In performing the upgrade, FalconStor acted in bad faith, and unfairly, by improperly using ANS's SAN as a virtual laboratory for trying untested methods and code to attempt to resolve the problems that affected Controller 2 during the upgrade and, even worse, by disregarding ANS's express instruction to refrain from rebooting the SAN until ANS cleanly shut down its systems.

113. As a direct and proximate result of FalconStor's breaches of the implied covenant of good faith and fair dealing in the Evaluation Agreement and in the Statement of Work, ANS experienced a devastating system failure and loss of client data, which in turn caused Plaintiffs to suffer significant damages.

114. Plaintiffs timely bring this claim against FalconStor to seek relief for the damages FalconStor's breaches of the implied covenant of good faith and fair dealing have caused.

115. Plaintiff ANS therefore is entitled to damages in an amount to be proven at trial.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for relief as follows:

(A) That the Court enter judgment awarding Plaintiffs damages against Defendant FalconStor Software, Inc. for all economic, monetary, actual, consequential, and compensatory damages Plaintiffs suffered as a result of FalconStor's conduct, together with pre- and post-judgment interest at the maximum rate allowable by law;

(B) That the Court award Plaintiffs exemplary or punitive damages against FalconStor to the extent allowable by law;

(C) That the Court award Plaintiffs their costs of suit, including reasonable attorneys' fees and expenses; and

(D) That the Court award such other and further relief as the Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs respectfully demand a trial by jury of all issues so triable.

Dated: July 18, 2012

Respectfully submitted,

LIEFF, CABRASER, HEIMANN & BERNSTEIN, LLP

By: _____
Jonathan D. Selbin

Jonathan D. Selbin (JS3097)
Michael J. Miarmi (MM1193)
250 Hudson Street, 8th Floor
New York, New York 10013-1413
Telephone: (212) 355-9500
Facsimile: (212) 355-9592
jselbin@lchb.com
mmiarmi@lchb.com

Eric B. Fastiff
(will seek admission *pro hac vice*)
275 Battery Street, 29th Floor
San Francisco, CA 94111-3339
Telephone: (415) 956-1000
Facsimile: (415) 956-1008
efastiff@lchb.com

Attorneys for Plaintiffs